Intelligence agencies eye the watch list dilemma

By Wilson P. Dizard III, GCN Staff

"Every couple of years this idea of the 'biometric magic bullet' resurfaces ... [but] identifying individuals is a daunting task."

—Jack Hermansen, Language Analysis Systems Inc.

Image: Rick Steele

Officials want to add biometrics and better search capabilities, but doubts persist about feasibility—and even possibility

Federal intelligence agencies want to improve their terrorist watch lists, at least partly through a tricky move toward biometrics.

"Now, it is a name-based system," said Michael Resnick, FBI supervisory special agent with the National Counter Terrorism Center, referring to the government's system for nominating people to the terror watch list and compiling information about them. "We are working on eventually moving it to a biometric system."

But some specialists in watch list technology warn that trying to shift to biometric systems poses insurmountable technical and business process obstacles.

In addition to the biometric move, the intelligence agencies want to add federated search capabilities that their analysts can use to merge information from dozens of databases.

Drawing closer

What's not in a name?

Databases that rely solely on name recognition have been relatively easy to get past.

"In other countries, many people understand very well how our writing system works and how easily our computers can be fooled because of the different ways that their names can be spelled when using our alphabet," said Jack Hermansen of Language Analysis Systems Inc.

"That is how Mir Aimal Kansi circumvented U.S. visa and border checks. He merely dropped the "n" in his surname, and our archaic name search system was unable to match the two slightly different names,"

Most Read Articles on GCN.com

Past 24 hours | Last 7 Days | Last 30 Days

- VA gets IT reorganization under way
- More Microsoft browser vulnerabilities reported
- GAO report hits HHS IT security flaws
- NARA puts over 400,000 State Department records online
- New Jersey CTO steps down

Go to complete list

Most E-Mailed Articles on GCN.com

Past 24 hours | Last 7 Days | Last 30 Days

- VA CIO resigns over pace of IT change
- Managers who put plans into action
- Biometrics look ready for prime time
- Lessons learned: SSL VPN
- Enterprise efforts are in tune at USDA

Go to complete list

Hermansen said.

Kansi subsequently shot five people in front of CIA headquarters in 1993, a crime for which he was executed in November 2002.

This search capability could access vast troves of biometric information, primarily in the form of fingerprints, in its existing databases, Resnick said recently at the E-Gov Institute's Security Conference in Washington.

The intelligence community has opportunities to supplement those biometric resources with other methods, such as retinal scans, according to Resnick.

"We are working on it currently. We have a tremendous amount of information in the federal family," he said, referring not only to biometric data, but also to information that could be accessed by a federated search system.

Resnick cited the government's vast array of databases containing communications intercepts, geospatial data, satellite images, human intelligence, open-source information and the like.

But trying to migrate terrorist watch lists to biometric identifiers could be overambitious, said Jim Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington.

"Biometric data is more reliable than names," Lewis conceded. "We don't even know how to spell these names sometimes."

But "the problem is that it is a lot easier to collect names than biometric data. You can get biometric data [only] if you control people or if they volunteer it," he said.

By contrast, asking for a DNA sample every time a traveler applies for a passport or visa would be impractical and, most likely, inefficient, Lewis said. "The bigger concern is that it doesn't get you the people you don't know about."

Another specialist in name analysis and matching systems echoed Lewis' concerns.

"Every couple of years, this idea of the 'biometric magic bullet' resurfaces," said Jack Hermansen, chief executive officer of Language Analysis Systems Inc. of Herndon, Va., in an e-mail response.

"Usually, it is followed by the sobering realization that identifying individuals is a daunting task requiring an operation dedicated to training, procedures and contingency plans that overwhelm those attempting to envision how to implement such an operation."

Hermansen said biometrics gives the intelligence community a false hope that biometric identifiers could solve the problems of finding terrorists.

Lewis noted that intelligence information usually provides names of people, such as those at clandestine meetings. But getting biometric information on those people would be much harder.

"For a long time to come, perhaps forever, you won't have the data to depend entirely on a biometric system," Lewis said. "But there will be

some cases where, if you have a name that triggers interest, you go back and look for biometric information."

Hermansen pointed to problems such as the inability of biometric systems to aid identification the first time the gov- ernment encounters an individual, and the fact that biometric look-ups do not provide information about how to broaden or narrow searches.

The notion of a fingerprint "close to" another fingerprint is meaningless, he said.

Biometric databases also don't do well with data that has been purposely altered, such as a deliberately misspelled name, Hermansen said.

Despite the shortcomings, name recognition and biometric techniques can work very well together to identify people, Hermansen said, particularly with "trusted" individuals who have volunteered their information.

The prospects for developing federated search capabilities appear closer to realization than a fully biometric watch list, partly because federal officials have been working for years to exploit the potential of merging information from different sources.

Resnick said a federated search capability would let analysts burrow through huge databases to tease out the relevant facts about individuals.

"The trick is to have these interconnect, so as to have federated searches," he said.

He cited efforts by the Justice and Homeland Security departments to coordinate information held in the FBI's Integrated Automated Fingerprint Iden- tification System with DHS' IDENT database inherited from the Immigration and Naturalization Service.

Homeland Security secretary Michael Chertoff announced this summer that IDENT would be shifted to accept 10 fingerprints rather than two, bringing it closer to compatibility with IAFIS.

One top-secret database the NCTC uses is called the Terrorist Identities Determinant Environment, known as TIDE. It provides a snapshot of everything known about individual terrorists.

A special advantage of TIDE, in contrast to other classified databases, is that it is classified down to the field level, Resnick said.

As a result, users can filter out secret or top-secret data fields relating to a person when they distribute a record at the "For Official Use Only" level, which is equivalent to the "law enforcement confidential" classification level used by state and local agencies.

According to Resnick, before Sept. 11, 2001, federal terrorist databases included only four data fields. Now they have been expanded to 40.

NCTC's terrorist watch list database now includes additional fields for aliases, physical descriptions of a person, phone numbers related to the person and the like, Resnick said.

"We are constantly trying to evolve our records," Resnick said.

More news on related topics: Biometrics, Homeland Security, Identity Management, Management